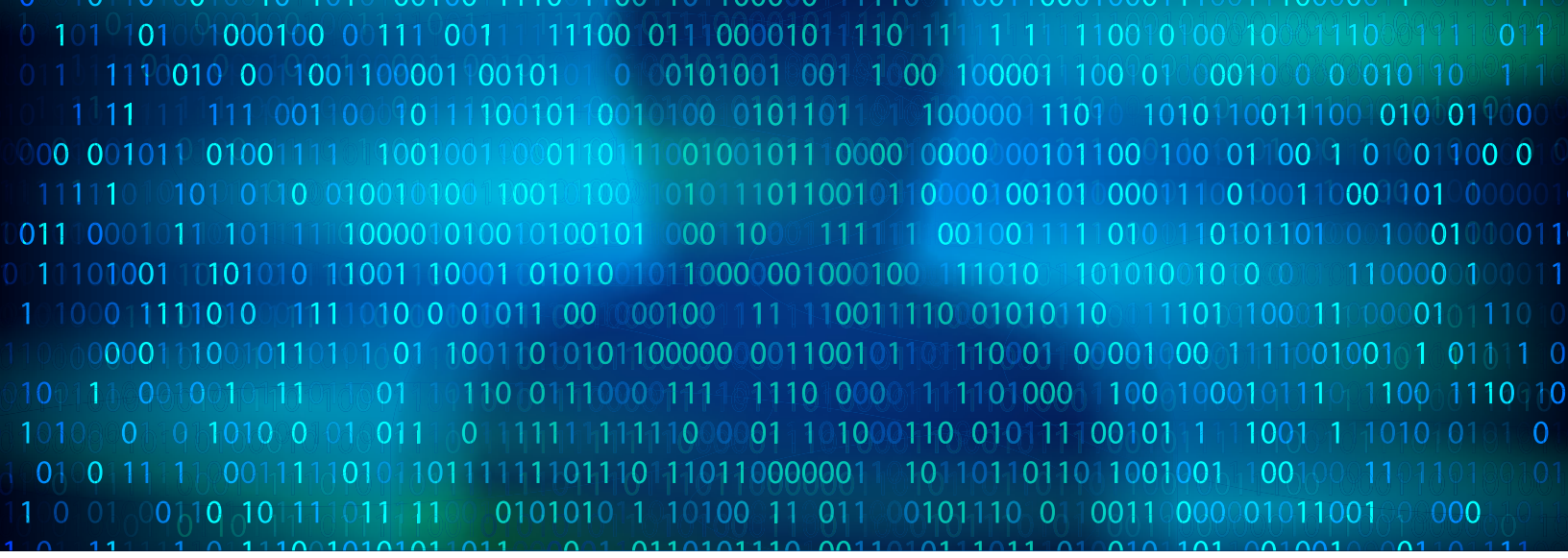




Reactive Security Leaves You In The Dark

WHITE PAPER

Dan Woods



CONTENTS

The Modern Problem of Cyber Security Defense	3
The Ideal State	5
The Benefits of the Ideal State	10
Conclusion	11

It is far better to operate with a mindset that prioritizes learning as much as possible about threats and your environment, and then proactively apply those lessons in your war against your adversaries.

THE MODERN PROBLEM OF CYBER SECURITY DEFENSE

Currently, in most companies, security is built around a combination of human oversight and technology. In essence, security teams made up of threat intelligence analysts, security operations professionals, and incident responders use technology to protect their organizations from threats. Great strides have been made to modernize the cyber security defense processes and procedures these security professionals follow. However, the unfortunate consequence is that many leaders now challenge their teams to improve metrics like Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR) without also rewarding teams for expanding their knowledge of the threats and applying that knowledge systematically to improve their company's overall security posture. This narrow focus on tactical and operational metrics fosters a reactive approach (which leaves security professionals numb and at times overwhelmed) rather than a strategic approach where the goal is to understand the adversary and fight smarter in the cyber security war.

It is time for a renaissance for cyber security defense. With well-defined processes and procedures, it's time for your team to lift their heads and focus on learning. To facilitate this change, empower security professionals with visibility to the battlefield where threats operate and challenge them to learn, iterate together, and improve your security posture. It is far better to operate with a mindset that prioritizes learning as much as possible about threats and your environment, and then proactively apply those lessons in your war against your adversaries.

This paper will examine ways to transform your security efforts, advancing from a tactical approach of reacting to threats to a strategic approach that increases the efficiency and effectiveness of your cyber security defense.

The Evolution of Cyber Security Defense

Mounting Challenges



**TOOL
PROLIFERATION**



**MYRIAD
OF DATA
FORMATS**



**DATA
INTEGRATION
CHALLENGES**



**SILOED SYSTEMS
/UNEVEN
COVERAGE**



**SWIVEL CHAIR
MANUAL
EFFORTS**



**FALSE
POSITIVES**

Cyber security defense continues to be challenging

Recent Advancements



**REPEATABLE
RESPONSE
PROCESSES**



**DEFINED
ESCALATION
PATHS**



**CLEARLY DEFINED
TACTICAL
METRICS**

Teams have made operational and tactical advancements

Current State



REACTIVE



BLINDSPOTS



**EFFICIENCY &
EFFECTIVENESS
STILL A STRUGGLE**



**HIT A WALL
IMPROVING
MTTD & MTTR**



**ADVERSARIES
STILL
WINNING**

And while there are improvements, we still have room to improve

Providing security professionals with pervasive visibility through packet brokers and agents is akin to ensuring your army is in the right place for battle. If you don't give them visibility, you can't expect them to win.

THE IDEAL STATE

Companies need an approach to cyber security that is strategic rather than simply tactical and operational. Whatever methodology is currently in use, ask yourself, "What is the goal of cyber security defense?" A tactical goal is to identify a threat and mitigate it as quickly as possible. A strategic goal looks to gain ground in addition to responding effectively to the current threat, changing the game over time.

As You Move From Tactical to Strategic

Tactical	Strategic
We are losing the battle.	We are a target; we have or will be breached.
We don't know what we don't know.	We've learned how threats operate and are using that to our advantage.
We fear becoming a headline.	We strategically and iteratively gain visibility across our enterprise.

The ideal state requires two things: 1) ensuring that security professionals have visibility to the actual battlefield where threats operate and are armed for battle with the right equipment; 2) providing security professionals with the right strategy to win the war.

The Attackers' Battlefield

You can't stop what you can't see. Threat actors leverage custom tools and exploits along with seemingly benign native network and system capabilities to compromise software and systems of all types, traverse your network, and exfiltrate data or cause damage. Their battlefield is your network and all the IP-enabled hosts and devices on it.

For security professionals to combat attackers, they must have visibility across the entire battlefield. Fortunately technology has advanced to give security professionals pervasive visibility into your network and endpoints. For example, today's intelligent packet brokers can aggregate all your cloud and network traffic (including all east-west traffic), deduplicate packets, perform network and application layer filtering, and decrypt SSL traffic. Similarly, software agents can reside on IP-enabled devices and intercept all the actions taken on a specific host. Providing security professionals with pervasive visibility through packet brokers and agents is akin to ensuring your army is in the right place for battle. If you don't give them visibility, you can't expect them to win.

Now that your security professionals have visibility to the battlefield, you must arm them with the ability to study and learn. Unfortunately, it is impractical to believe that we can always stop attackers in real-time, so security professionals need the ability to play back surveillance footage to rapidly zero in on suspicious activity. Both Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) security tools now record in-depth metadata about everything they observe so that security professionals are not only able to hunt or detect malicious activity, but also to piece together the movements and behaviors of their adversaries.

The Right Strategy

There are numerous excellent methodologies, processes, and procedures that can be followed by security professionals, but they are primarily tactical in nature. Most lack a core strategy that encourages security professionals, whatever their focus (threat intelligence, threat hunters and security operations, or incident response) to learn from what they observe and steadily make improvements to your security posture.

We recommend embracing a high-level mental model of Understand | Observe | Discover that serves to facilitate cross-team collaboration, learning, and ultimately stronger cyber security defense. Here are the three elements of this model.



We recommend a high-level mental model of Understand | Observe | Discover that serves to facilitate cross-team collaboration, learning, and ultimately stronger cybersecurity defense.

Understand

Meaning: A deep understanding of your adversaries, their capabilities, their intentions, their tools, their infrastructure, how they behave, and what to prioritize.

Team: 'Understand' traditionally aligns with a cyber security defense program's Threat Intelligence team, but should enlist cross-functional contributions from Hunters, Analysts, and Responders in the Security Operations and Incident Response teams.

Benefit: By studying the behavior of active threats in your network, security professionals can focus on threats that are targeting them, learn from them, and iterate together on prevention and detection mechanisms.

Aggregating Intelligence Data

To make the most use of the intelligence data you gather from studying threats, threat actors, and malware, store the information in a Threat Intelligence Platform (TIP) or a custom knowledge base designed to capture the information and map it to a threat model. Associating the technical components of an attacker's behaviors with the [Mitre ATT&CK](#) model can also help by mapping them to a common taxonomy that improves communication about threats inside and outside your organization.

Observe

Meaning: Utilize security tooling (EDR and NDR) to apply your newly acquired understanding of threats and seek them out in your battlefield.

Team: Observation is carried out by Hunters and Analysts in the Security Operations team. With visibility to the battlefield and equipped with EDR and NDR tools, analysts perform surveillance and identification of threats. It is important that your Threat Intelligence and Incident Response teams also have observational capabilities to enable their learning and discovery.

Benefit: Faster threat identification. Endpoint observations of threats provide depth into a specific event on a specific host. Network observations provide insight into the breadth and scale of the threat

such as what occurred prior to an incident, how the threat spread throughout the network, and the risk associated with the threat. Both types of observations facilitate discovery.

Discover

Meaning: Leveraging your organization's understanding of the threats and your ability to observe to detect your adversaries, respond to mitigate the threats, and collaborate to iteratively expand your understanding of your enemy.

Team: Discover encompasses both Hunters and Analysts in the Security Operations team, whose job is to track down and detect threats, and the Incident Response team, whose job is to triage the severity of an attack and direct reactive combat to minimize the risk of the threat. However, the Threat Intelligence team also plays a role in ensuring that all the new knowledge obtained about your adversary during the attack is captured and learned from.

Benefit: Tactically, Discover will reduce your MTDD and MTTR, but strategically, Discover must loop back to improve your ability to understand, which in turn enables you to protect your organization and win the battle by:

- Applying new prevention and detection mechanisms to rapidly identify threats with comprehensive network visibility.
- Utilizing knowledge of attackers and context of their behaviors to properly respond and reduce risk.
- Investigating the root cause of an event and collecting, consolidating, and retaining enriched metadata and context around all activity and devices related to an event.
- Creating a repeatable process that relies on smooth cross-team collaboration so that threats can be handled systematically.

By embracing the mental model of Understand | Observe | Discover, companies can create a cyber security defense program that empowers and challenges security teams to expand their knowledge, which in turn increases their efficiency and decreases ineffective use of their time (chasing false positives, swivel chair manual efforts, and so on).

Once this occurs, companies can start asking questions on a larger scale and identifying systematic weaknesses or strengths in their overall security posture, as well as validating where things need to change. This

If we pursue a strategic approach to cyber security defense, ultimately, we can shift the balance of power from the attackers to the defenders.

simply isn't possible if companies don't have robust visibility into their networks and endpoints, the tools to perform proper surveillance and investigations, and the mental model to always be learning.

THE BENEFITS OF THE IDEAL STATE

The ideal state offers benefits that are difficult to achieve otherwise.

Cyber security confidence. Most companies have an inaccurate perception of their organizational security posture, leading to unfounded confidence or fear.

There is nothing more dangerous for a CISO than to think that the business is secure when in reality it is not. An iterative approach of Understand | Observe | Discover means your security posture isn't just measured by things such as MTTD and MTTR, but also by knowledge gained and applied. The result is constant learning about the reality of your current posture and a mechanism for improvement.

Empowered security professionals. As companies move closer to this ideal state, security professionals experience a number of downstream benefits:

- Reduced alert fatigue, less downtime due to updates, reduction in obstacles to efficiency and increased job satisfaction.
- Faster investigations as experience is gleaned and applied.
- Continuous learning that benefits the entire cyber security defense program and offers improved efficiency and effectiveness.
- Increased collaboration among teams and improved morale.

CONCLUSION

The next step in improving cyber security defense requires security leaders to enable and encourage their teams not just to make tactical and operational improvements but also to focus on gaining and applying knowledge.

Get your security professionals onto the same battlefield as the attackers through pervasive network visibility (using intelligent packet brokers) and endpoint visibility (software agents). Suit them up for battle with investigative tools such as Endpoint Detection and Response and Network Detection and Response. Ensure their success by providing them with the right strategy to win the war, which means challenging them to continuously learn and improve your security posture rather than measuring them solely on metrics like Mean Time to Detect and Mean Time to Respond.

If we pursue a strategic approach to cyber security defense, ultimately, we can shift the balance of power from the attackers to the defenders.

This paper was written by Dan Woods and sponsored by Gigamon. Learn more about [Gigamon](#) or request a [personalized demo](#).

Connect with us



© 2019 Early Adopter Research

